

#2

Docket No. 1614.1040/HJS

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

jc525 U.S. PTO  
09/531105  
03/17/00

In re Application of:

Shinkichi GAMA et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: March 17, 2000

For: STORAGE DEVICE

**SUBMISSION OF CERTIFIED COPY OF PRIOR  
FOREIGN APPLICATION IN ACCORDANCE WITH  
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application(s):

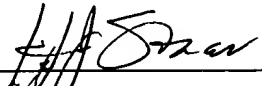
Japanese Patent Application No. 11-195527  
Filed: July 9, 1999

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date, as evidenced by the certified papers attached hereto, in accordance with the requirements  
of 35 U.S.C. § 119.

Respectfully submitted,  
STAAS & HALSEY LLP

Date: March 17, 2000

By: \_\_\_\_\_

  
H. J. Staas  
Registration No. 22,010

700 Eleventh Street, N.W.  
Suite 500  
Washington, D.C. 20001  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

Jc525 U.S. PTO  
09/531105  
03/17/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 9 年 7 月 9 日

出 願 番 号

Application Number:

平成 1 1 年特許願第 1 9 5 5 2 7 号

出 願 人

Applicant (s):

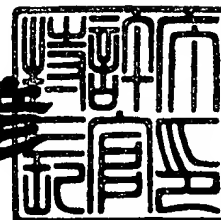
富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 0 年 2 月 1 4 日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特 2 0 0 0 - 3 0 0 6 3 5 2

【書類名】 特許願

【整理番号】 9950685

【提出日】 平成11年 7月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明の名称】 メモリ装置

【請求項の数】 9

【発明者】

    【住所又は居所】 神奈川県横浜市港北区新横浜二丁目 1 5 番 1 6 株式会  
社富士通コンピュータテクノロジー内

    【氏名】 蒲 信吉

【発明者】

    【住所又は居所】 神奈川県横浜市港北区新横浜二丁目 1 5 番 1 6 株式会  
社富士通コンピュータテクノロジー内

    【氏名】 柴崎 省吾

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100095072

    【弁理士】

    【氏名又は名称】 岡田 光由

    【電話番号】 03-3807-1818

【選任した代理人】

    【識別番号】 100074848

    【弁理士】

    【氏名又は名称】 森田 寛

【手数料の表示】

    【予納台帳番号】 012944

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707817

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メモリ装置

【特許請求の範囲】

【請求項 1】 電源遮断時にもデータを保持するとともに、テスト端子から入力されるテスト信号に従ってテスト処理を実行するメモリ装置であって、

秘匿データを格納するメモリに対して、データの読み出し指示を発行する発行手段と、

上記発行手段の発行処理に応答して読み出されるデータから、上記メモリに秘匿データが格納されているのか否かを解読する解読手段と、

上記解読手段の解読結果を揮発性の形態で保持する保持手段と、

上記保持手段が秘匿データの格納を示す情報を保持するときに、テスト端子から入力されるテスト信号を遮断する遮断手段とを備えることを、

特徴とするメモリ装置。

【請求項 2】 請求項 1 記載のメモリ装置において、

発行手段は、秘匿データを格納するメモリに対して、秘匿データの読み出し指示を発行することを、

特徴とするメモリ装置。

【請求項 3】 請求項 1 記載のメモリ装置において、

発行手段は、秘匿データを格納するメモリに対して、それが格納する作業用データを除く全てのデータの読み出し指示を発行することを、

特徴とするメモリ装置。

【請求項 4】 請求項 1 記載のメモリ装置において、

発行手段は、秘匿データを格納するメモリに対して、秘匿データの格納に用いられない領域に格納される秘匿データの格納の有無を示すデータの読み出し指示を発行することを、

特徴とするメモリ装置。

【請求項 5】 請求項 1 ～ 4 に記載されるいずれかのメモリ装置において、

発行手段は、電源投入時に、データの読み出し指示を発行することを、

特徴とするメモリ装置。

【請求項 6】 請求項 1～5 に記載されるいずれかのメモリ装置において、発行手段は、リセット時に、データの読み出し指示を発行することを、特徴とするメモリ装置。

【請求項 7】 請求項 1～5 に記載されるいずれかのメモリ装置において、発行手段は、秘匿データを操作するコマンドの発行時に、データの読み出し指示を発行することを、特徴とするメモリ装置。

【請求項 8】 電源遮断時にもデータを保持するとともに、テスト端子から入力されるテスト信号に従ってテスト処理を実行するメモリ装置であって、

秘匿データを格納するメモリに対してのアクセス要求の発行に応答して読み出されるデータを収集し、その収集データから該メモリに秘匿データが格納されているのか否かを解読する解読手段と、

上記解読手段の解読結果を揮発性の形態で保持する保持手段と、

上記保持手段が秘匿データの格納を示す情報を保持するときに、テスト端子から入力されるテスト信号を遮断する遮断手段とを備えることを、

特徴とするメモリ装置。

【請求項 9】 電源遮断時にもデータを保持するとともに、テスト端子から入力されるテスト信号に従ってテスト処理を実行するメモリ装置であって、

秘匿データを格納するメモリに対してのアクセス要求が発行されるときに、その旨を示す情報を揮発性の形態で保持する保持手段と、

上記保持手段がアクセス要求の発行を示す情報を保持するときに、テスト端子から入力されるテスト信号を遮断する遮断手段とを備えることを、

特徴とするメモリ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電源遮断時にもデータを保持するメモリ装置に関し、特に、高いセキュリティを実現しつつ、テスト端子から入力されるテスト信号に従ってテスト処理を実行できるようにするメモリ装置に関する。

【0002】

メモリ装置に格納されるデータのセキュリティを確保することは非常に重要なことである。一方、メモリ装置の品質を向上させることも非常に重要なことである。

【0003】

メモリ装置の品質を向上させるには、製造されたメモリ装置をテストして故障のあるものを検出していく必要がある。しかるに、このようなテストを可能にすべくテスト用の端子を設けると、不正使用者がこのテスト機能を利用することで、メモリ装置に格納される暗号キーなどの秘匿データを取得できる可能性がでてくる。

【0004】

これから、高いセキュリティを実現しつつ、製造されたメモリ装置をテストできるようにする技術を構築していく必要がある。

【0005】

【従来の技術】

例えば、メモリスティックなどのような不揮発性メモリに、暗号化された音楽などの著作物を記録することが行われている。

【0006】

このような場合に、暗号キーがハックされると、その著作物が無断でコピーされてしまうという不都合が起こる。

【0007】

また、不揮発性メモリとその不揮発性メモリを利用するホスト装置との間で、共通鍵の暗号キーを使って暗号文をやり取りすることで、認証処理を実行するということが行われている。

【0008】

このような場合にも、暗号キーがハックされると、不正使用者の操作するホスト装置が不揮発性メモリのデータを参照できることになるという不都合が起こる。

【0009】

そこで、従来では、不正使用者がテスト機能を使って暗号キーなどの秘匿データを盗めないようにするために、メモリスティックなどのような不揮発性メモリにはテスト用端子を設けないようにする構成を採っている。

【0010】

【発明が解決しようとする課題】

確かに、従来技術のように、不揮発性メモリにテスト用端子を設けないようにすれば高いセキュリティを確保できるようになる。

【0011】

しかしながら、それでは、不揮発性メモリの製造メーカは、製造された不揮発性メモリを十分にテストすることができず、その品質を保証することができない。

【0012】

これから、従来技術に従っていると、メモリスティックなどのような不揮発性メモリの品質を向上させることができないという問題点があった。

【0013】

本発明はかかる事情に鑑みてなされたものであって、電源遮断時にもデータを保持する構成を採るときにあって、高いセキュリティを実現しつつ、テスト端子から入力されるテスト信号に従ってテスト処理を実行できるようにする新たなメモリ装置の提供を目的とする。

【0014】

【課題を解決するための手段】

図1に本発明の原理構成を図示する。

【0015】

図中、1は本発明を具備するメモリ装置であって、電源遮断時にもデータを保持するとともに、テスト端子から入力されるテスト信号に従ってテスト処理を実行するものである。

【0016】

本発明のメモリ装置1は、秘匿データメモリ手段10と、回路手段11-i ( $i = 1 \sim n$ ) と、テスト入力用インタフェース手段12と、遮断手段13と、発行



手段 14 と、解読手段 15 と、保持手段 16 とを備える。

【0017】

この秘匿データメモリ手段 10 は、暗号キーなどの秘匿データを格納し、秘匿データを格納しないときには、秘匿データとは異なる初期データを格納し、秘匿データを格納するときにあつて、秘匿データを格納する領域以外の領域があるときには、その領域に、秘匿データの格納の有無を示すデータを格納することがある。

【0018】

回路手段 11-i ( $i = 1 \sim n$ ) は、秘匿データメモリ手段 10 から秘匿データを読み出し、それを使って規定の処理を実行する。テスト入力用インタフェース手段 12 は、テスト端子から、回路手段 11-i ( $i = 1 \sim n$ ) のテストに用いるテスト用信号を入力する。遮断手段 13 は、テスト入力インタフェース手段 12 の入力するテスト信号を遮断する。

【0019】

発行手段 14 は、秘匿データメモリ手段 10 に対してデータの読み出し指示を発行する。解読手段 15 は、秘匿データメモリ手段 10 から読み出されるデータを解読することで、秘匿データメモリ手段 10 に秘匿データが格納されているのか否かを解読する。保持手段 16 は、解読手段 15 の解読結果を揮発性の形態で保持する。

【0020】

このように構成される本発明のメモリ装置 1 では、発行手段 14 は、電源投入時に、秘匿データメモリ手段 10 に対してデータの読み出し指示を発行したり、リセット時に、秘匿データメモリ手段 10 に対してデータの読み出し指示を発行したり、秘匿データを操作するコマンドの発行時に、秘匿データメモリ手段 10 に対してデータの読み出し指示を発行する。

【0021】

このとき、発行手段 14 は、秘匿データメモリ手段 10 に対して、秘匿データの読み出し指示を発行したり、作業用データを除く全てのデータの読み出し指示を発行したり、秘匿データの格納に用いられない領域に格納される秘匿データの

格納の有無を示すデータの読み出し指示を発行する。

【0022】

この発行手段14の発行処理を受けて、秘匿データメモリ手段10は、秘匿データを格納するときには、秘匿データや秘匿データの格納を示すデータを出力し、秘匿データを格納しないときには、秘匿データとは異なる初期データや秘匿データの未格納を示すデータを出力し、これを受けて、解読手段15は、秘匿データメモリ手段10に秘匿データが格納されているのか否かを解読する。

【0023】

この解読手段15の解読結果を受けて、保持手段16は、秘匿データメモリ手段10に秘匿データが格納されているのか否かを示す情報を保持し、これを受けて、遮断手段13は、保持手段16が秘匿データの格納を示す情報を保持するときには、テスト入力用インタフェース手段12から入力されるテスト信号を遮断する。

【0024】

このようにして、本発明のメモリ装置1では、秘匿データメモリ手段10に秘匿データが格納されているときには、テスト信号の入力を受け付けないことでテストできないようにする構成を採ることから、実質的にテスト端子を持たないメモリ装置と同等のセキュリティを実現しつつ、品質向上のためのテストを実行できるようになる。

【0025】

一方、このように構成される本発明のメモリ装置1では、秘匿データメモリ手段10に対してアクセス要求が発行されると、解読手段15は、そのアクセス要求に応答して秘匿データメモリ手段10から読み出されるデータを収集して、その収集データから秘匿データメモリ手段10に秘匿データが格納されているのか否かを解読する。

【0026】

この解読手段15の解読結果を受けて、保持手段16は、秘匿データメモリ手段10に秘匿データが格納されているのか否かを示す情報を保持し、これを受けて、遮断手段13は、保持手段16が秘匿データの格納を示す情報を保持すると

きには、テスト入力用インタフェース手段 1 2 から入力されるテスト信号を遮断する。

【 0 0 2 7 】

ここで、保持手段 1 6 は、秘匿データメモリ手段 1 0 に対してアクセス要求が発行されるときに、その旨を示す情報を保持し、これを受けて、遮断手段 1 3 は、直ちに、テスト端子から入力されるテスト信号を遮断する構成を採ることも可能である。

【 0 0 2 8 】

このようにして、本発明のメモリ装置 1 では、秘匿データメモリ手段 1 0 に対するアクセス要求の発行を検出すると、それ以降、テスト信号の入力を受け付けないようにする構成を採ることから、実質的にテスト端子を持たないメモリ装置と同等のセキュリティを実現しつつ、品質向上のためのテストを実行できるようになる。

【 0 0 2 9 】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【 0 0 3 0 】

図 2 に、本発明の一実施例を図示する。

【 0 0 3 1 】

図中、2 0 は本発明を具備するメモリスティック、3 0 はメモリスティック 2 0 を利用するホスト装置である。

【 0 0 3 2 】

本発明のメモリスティック 2 0 は、フラッシュメモリ 4 0 と、フラッシュメモリ 4 0 をコントロールする M S コントローラ 5 0 とで構成されており、ホスト装置 3 0 から、シリアルプロトコルバスステート信号 ( B S ) とシリアルプロトコルクロック信号 ( S C L K ) とを入力し、ホスト装置 3 0 との間で、シリアルプロトコルデータ信号 ( D I O ) をやり取りする。

【 0 0 3 3 】

この M S コントローラ 5 0 は、ホスト装置 3 0 との間のインタフェース処理を

司るホストインタフェース 51 と、フラッシュメモリ 40 との間のインタフェース処理を司るフラッシュインタフェース 52 と、レジスタ 53 と、ページバッファ 54 と、ROM 55 と、コントローラ用メモリ 56 と、暗号復号機構 57 と、セキュリティ機構 58 とを備える。

【0034】

図 3 に示すように、暗号復号機構 57 は、暗号復号回路 570 と乱数発生回路 571 とを備え、コントローラ用メモリ 56 は、例えば 512 バイトで構成されて、例えば 16 バイトで構成される複数の暗号キーを格納する暗号キーメモリ域と、乱数発生回路 571 の発生する乱数などを格納するために用意される作業用メモリ域とを備える。

【0035】

ここで、暗号キーが格納されてない場合には、このコントローラ用メモリ 56 の暗号キーメモリ域には、暗号キーとして用いられることのないオール 0 などのような規定の初期データが格納されることになる。

【0036】

このように構成される暗号復号機構 57 では、ホスト装置 30 との間でデータをやり取りする必要があると、乱数発生回路 571 が乱数を発生して、これを暗号復号回路 570 に通知するとともに、コントローラ用メモリ 56 の作業用メモリ域に格納する。

【0037】

この乱数発生回路 571 から通知される乱数を受けて、暗号復号回路 570 は、コントローラ用メモリ 56 の暗号キーメモリ域から、その乱数の指定する暗号キーを読み出し、通知された乱数をキーにして、その読み出した暗号キーを暗号化してホスト装置 30 に送信する。

【0038】

この MS コントローラ 50 からの暗号文を受け取ると、ホスト装置 30 は、暗号文を解読することで、暗号復号回路 570 の読み出した暗号キーを知ることができるので、その暗号キーを使って必要なデータを暗号化して MS コントローラ 50 に返信する。

【0039】

そして、このホスト装置30からの暗号文を受け取ると、暗号復号回路570は、自分の用いた暗号キーを使ってこの暗号文を復号することで、ホスト装置30の返信してきたデータを解読する。

【0040】

このようにして、MSコントローラ50は、共通鍵となる暗号キーを用いて、ホスト装置30との間で暗号文のやり取りを行っていくが、認証処理などのような場合には、安全性を高めるために、複数の暗号キーを使って暗号文をやり取りする必要がある。このような場合には、乱数発生回路571は、コントローラ用メモリ56の作業用メモリ域に格納した前回の発生乱数を読み出して、それに基づいて次の乱数を発生していくことで、発生する乱数のランダム性を確保していくように処理している。

【0041】

このような処理を行うMSコントローラ50を持つメモリスティック20の品質を保証するためには、MSコントローラ50が設計通りに製造されているの可否かをテストしていく必要がある。しかるに、このようなテスト機能を持つと、それを利用して、不正使用者が暗号キーを盗み取る可能性がででくる。

【0042】

そこで、MSコントローラ50は、このような可能性を排除するために、図2に示したようにセキュリティ機構58を備える構成を採っている。

【0043】

図4に、このセキュリティ機構58の一実施例を図示する。ここで、図中の56は図2に示したコントローラ用メモリ、570は図3に示した暗号復号回路、571は図3に示した乱数発生回路571である。

【0044】

この図に示すように、セキュリティ機構58は、シーケンサ580と、テスト入力インタフェース581と、テストセレクト部582と、内部信号セレクト出力部583と、レジスタ584と、デコーダ585と、制御フラグラッチ回路586とを備える。

【0045】

このシーケンサ580は、電源投入を契機として起動されて、全体の制御処理を実行する。テスト入力インタフェース581は、テスト端子から入力されてくるテスト信号を入力し、それをデコードすることで対応するテスト機能と呼び出す。

【0046】

テストセレクト部582は、制御フラグラッチ回路586にラッチされる制御フラグに従って、テスト入力インタフェース581の出力するテスト信号を遮断するの否かを制御する。内部信号セレクト出力部583は、テスト出力をテスト端子に出力する。

【0047】

レジスタ584は、コントローラ用メモリ56から読み出されるデータ（暗号キーが格納されている場合には暗号キー、暗号キーが格納されていない場合には初期データ）を保持する。

【0048】

デコーダ585は、レジスタ584の保持するデータをデコードすることで、レジスタ584の保持するデータが暗号キーであるのかそれ以外の初期データであるのかをデコードする。制御フラグラッチ回路586は、デコーダ585のデコード結果をラッチしてテストセレクト部582を制御する。

【0049】

図5に、セキュリティ機構58の備えるシーケンサ580の一実施例を図示する。

【0050】

この図に示すように、シーケンサ580は、シーケンサ動作フラグON部5800と、シーケンサ・カウンタ5801と、シーケンサ動作終了信号生成部5802と、メモリアドレス生成部5803と、読出信号生成部5804と、レジスタ格納信号生成部5805とを備える。

【0051】

このシーケンサ動作フラグON部5800は、電源が投入されるときに、動作

フラグをONする。シーケンサ・カウンタ5801は、動作フラグがONしている間、計数値をカウントアップして、その計数値が規定値に到達するときに、メモリアドレス生成部5803／読出信号生成部5804／レジスタ格納信号生成部5805を起動する。シーケンサ動作終了信号生成部5802は、シーケンサ・カウンタ5801の計数値が最大値に到達するときに、動作フラグをOFFさせる動作終了信号を生成する。

#### 【0052】

メモリアドレス生成部5803は、暗号キーの格納先となっているコントローラ用メモリ56のメモリアドレスを生成する。読出信号生成部5804は、コントローラ用メモリ56からのデータの読み出しを指示する読出信号を生成する。レジスタ格納信号生成部5805は、レジスタ584の格納タイミング信号となるレジスタ格納信号を生成する。

#### 【0053】

このように構成されるセキュリティ機構58は、次に説明する動作を実行することで、不正使用者による暗号キーのハックを防止する。

#### 【0054】

すなわち、セキュリティ機構58の備えるシーケンサ580は、電源が投入されると、シーケンサ・カウンタ5801によるシーケンス動作に入って、先ず最初に、メモリアドレス生成部5803を起動することで、暗号キーの格納先となっているコントローラ用メモリ56のメモリアドレスを生成し、続いて、読出信号生成部5804を起動することで、コントローラ用メモリ56からのデータの読み出しを指示する読出信号を生成する。

#### 【0055】

このメモリアドレス及び読出信号の生成を受けて、コントローラ用メモリ56は、そのメモリアドレスの指定する例えば16バイトのデータを読み出していく。すなわち、暗号キーが格納されているときには暗号キー、暗号キーが格納されていないときには初期データを読み出していくのである。

#### 【0056】

続いて、シーケンサ580は、レジスタ格納信号生成部5805を起動するこ

とで、レジスタ 5 8 4 の格納タイミング信号となるレジスタ格納信号を生成する。

【 0 0 5 7 】

このレジスタ格納信号を受けて、レジスタ 5 8 4 は、コントローラ用メモリ 5 6 から読み出されたデータを保持する。

【 0 0 5 8 】

このようにして、レジスタ 5 8 4 に、コントローラ用メモリ 5 6 から読み出されたデータが保持されると、デコーダ 5 8 5 は、そのデータをデコードすることで、そのデータが暗号キーであるのかそれ以外の初期データであるのかをデコードし、これを受けて、制御フラグラッチ回路 5 8 6 は、レジスタ 5 8 4 に保持されるデータが暗号キーであるときには例えば 1 をラッチし、レジスタ 5 8 4 に保持されるデータが初期データであるときには例えば 0 をラッチする。

【 0 0 5 9 】

この制御フラグラッチ回路 5 8 6 のラッチする制御フラグを受けて、テストセレクト部 5 8 2 は、レジスタ 5 8 4 に保持されるデータが暗号キーであるときには、テスト入力インタフェース 5 8 1 の出力するテスト信号を遮断することでテスト機能の実行を阻止し、レジスタ 5 8 4 に保持されるデータが初期データであるときには、テスト入力インタフェース 5 8 1 の出力するテスト信号を遮断しないことでテスト機能の実行を阻止しないように処理する。

【 0 0 6 0 】

このようにして、セキュリティ機構 5 8 は、電源投入時にコントローラ用メモリ 5 6 に暗号キーが格納されているときには、それ以降、テストモードに入れないようにすることで、テスト機能を利用する暗号キーのハックを確実に防止するように処理するのである。

【 0 0 6 1 】

そして、セキュリティ機構 5 8 は、電源投入時にコントローラ用メモリ 5 6 に暗号キーが格納されていないときには、それ以降、テストモードに入れるようにすることで、MS コントローラ 5 0 が設計通りに製造されているのか否かをテストできるようにしている。



【0062】

すなわち、メモリスティック20の製造メーカは、MSコントローラ50をテストする場合には、ホスト装置30を使って、コントローラ用メモリ56に格納される暗号キーを消去した後、電源を一度切断してから再投入すれば、テストモードに入れるようになる。

【0063】

この構成を採るときに、セキュリティ機構58は、電源投入後に暗号キーが消去されることがあることを考慮して、リセットが発行されるときに上述した処理を実行することで、リセット発行時に暗号キーが消去されているときには、テスト入力インタフェース581の出力するテスト信号を遮断しないことでテスト機能の実行を阻止しないように処理する。

【0064】

メモリスティック20のユーザとなるメーカ（ユーザメーカ）から、コントローラ用メモリ56のどのメモリアドレス位置に暗号キーを格納するのかが知らされる場合には、メモリスティック20の製造メーカは、メモリアドレス生成部5803がそのメモリアドレスを生成するように設計する。

【0065】

しかしながら、ユーザメーカから、そのようなメモリアドレスが知らされない場合には、製造メーカは、メモリアドレス生成部5803がコントローラ用メモリ56から作業用データを除く全てのデータを読み出すことになるメモリアドレスを生成するように設計する。

【0066】

このときには、レジスタ584に、コントローラ用メモリ56から読み出されていくデータが順番に保持されていくことになるので、制御フラグラッチ回路586が暗号キーが読み出されたことを示す制御フラグをラッチするときに、レジスタ584に対して、それから以降のデータの保持を禁止させる処理を行う回路機構を用意することになる。

【0067】

上述したように、コントローラ用メモリ56の暗号キーメモリ域には、暗号キ

ーが格納されていない場合には、暗号キーとして用いられることのないオール 0 などのような規定の初期データが格納されることになる。

【0068】

これにより、暗号キーが格納されているのか格納されていないのかが判別できるようになるのであるが、メモリスティック 20 のユーザメーカによっては、メモリスティック 20 の製造メーカの想定した初期データを暗号キーとして使用する可能性もある。

【0069】

これから、ユーザメーカから、暗号キーとして使用することのないデータが知らされる場合には、製造メーカは、そのデータを初期データとして用いるように設計していくことになる。

【0070】

一方、ユーザメーカから、そのような初期データが知らされない場合には、製造メーカは、ユーザメーカに対して、コントローラ用メモリ 56 の作業用メモリ域の特定領域に、暗号キーの書き込みと同期させて、暗号キーの格納を示す特定のデータを書き込ませるように要求する。そして、その特定のデータを読み出して、デコーダ 585 によりデコードしていくことで、暗号キーが格納されているのか否かを判別するように設計していくようにする。

【0071】

図 4 の実施例では、電源が投入されるときに、コントローラ用メモリ 56 に暗号キーが格納されているのか否かを判断して、その判断結果を制御フラグラッチ回路 586 にラッチさせていくという構成を採った。そして、これに加えて、リセットが発行されるときに、コントローラ用メモリ 56 に暗号キーが格納されているのか否かを判断して、その判断結果を制御フラグラッチ回路 586 にラッチさせていくという構成を採ったが、その他のタイミング時に、この処理を行う構成を加えることも可能である。

【0072】

例えば、図 6 に示すように、セキュリティ機構 58 に発行コマンドを解釈するコマンド解釈部 587 を備える構成を採って、このコマンド解釈部 587 が暗号

キーを操作するコマンドの発行を検出するときに、コントローラ用メモリ 56 に暗号キーが格納されているのか否かを判断して、その判断結果を制御フラグラッチ回路 586 にラッチさせていくという構成を加えることも可能である。

【0073】

図 7 に、本発明を実現するためのセキュリティ機構 58 の他の実施例を図示する。

【0074】

図 4 の実施例では、電源投入時にコントローラ用メモリ 56 に暗号キーが格納されているときには、テストモードに入れないようにすることで、暗号キーのハックを防止する構成を採ったが、この実施例では、暗号復号回路 570 が暗号キーを読み出すときに、テストセレクト部 582 がテスト入力インタフェース 581 の出力するテスト信号を遮断するように動作させることで、テストモードに入っているときにはその継続を禁止させ、通常モードにあるときにはテストモードへの移行を禁止させていくという構成を採っている。

【0075】

暗号復号回路 570 が暗号キーを読み出すと、テスト機能を使って、その暗号キーをハックできる可能性が出てくるので、この構成に従って、そのような可能性を排除するのである。

【0076】

この実施例に従う場合、シーケンサ 580 は、図 8 に示すように、レジスタ格納信号生成部 5805 のみを備える構成を採って、このレジスタ格納信号生成部 5805 を使って、暗号復号回路 570 がコントローラ用メモリ 56 に格納される暗号キーのメモリアクセス信号を発行するときに、レジスタ 584 の格納タイミング信号となるレジスタ格納信号を生成するように処理する。

【0077】

このように構成される図 7 の実施例では、暗号復号回路 570 がコントローラ用メモリ 56 に対して暗号キーのアクセス信号を発行すると、シーケンサ 580 は、レジスタ格納信号生成部 5805 を起動することで、レジスタ 584 の格納タイミング信号となるレジスタ格納信号を生成する。

## 【0078】

このレジスタ格納信号を受けて、レジスタ584は、暗号復号回路570の読み出す暗号キーをサンプリングして保持する。

## 【0079】

このようにして、レジスタ584に暗号キーが保持されると、デコーダ585は、レジスタ584の保持するデータが暗号キーであることをデコードし、これを受けて、制御フラグラッチ回路586は、レジスタ584に保持されるデータが暗号キーであることを示す例えば1をラッチする。

## 【0080】

この制御フラグラッチ回路586のラッチする制御フラグを受けて、テストセレクト部582は、テスト入力インタフェース581の出力するテスト信号を遮断することでテスト機能の実行を阻止するように処理する。

## 【0081】

このようにして、この実施例に従う場合、セキュリティ機構58は、暗号復号回路570が暗号キーを読み出すと、それまでテストモードにあるときには、それ以降テストモードを継続させていかないように処理するとともに、それまで通常モードにあるときには、それ以降テストモードに入れないように処理することで、テスト機能を利用する暗号キーのハックを確実に防止するように処理するのである。

## 【0082】

図7の実施例では、暗号復号回路570の読み出す暗号キーをレジスタ584に保持させていくことで、制御フラグラッチ回路586に対して、テスト信号を遮断させるための制御フラグをラッチさせていくという構成を採ったが、図9に示すように、暗号復号回路570の発行する暗号キーのアクセス信号を受けて、シーケンサ580が直接制御フラグラッチ回路586に対して、テスト信号を遮断させるための制御フラグをラッチさせていくという構成を採ることも可能である。

## 【0083】

このようにして、図4の実施例に従う場合には、MSコントローラ50は、電

源投入時に、図10(a)の処理フローに示すように、コントローラ用メモリ56の暗号キーメモリ域からデータを読み出し、その読み出したデータが消去状態でない場合、すなわち、その読み出したデータが暗号キーである場合には、テスト信号の入力を遮断することで、テスト処理に入ることを禁止し、その読み出したデータが消去状態である場合には、テスト信号の入力を許可することで、テスト処理に入ることを許可していく構成を採るのである。

【0084】

この構成に従って、コントローラ用メモリ56に暗号キーが格納されている場合には、テストモードに入れないようにすることで、テスト機能を利用する暗号キーのハックを確実に防止できるようになる。

【0085】

一方、図7の実施例に従う場合には、MSコントローラ50は、暗号復号回路570が暗号キーのアクセス要求を発行するときに、図10(b)の処理フローに示すように、テスト信号の入力を遮断することで、テスト処理に入ることを禁止したり、テスト処理に入っているときは、その継続を禁止していく構成を採るのである。

【0086】

この構成に従って、コントローラ用メモリ56から暗号キーが読み出された場合には、テストモードに入れないようにしたり、テストモードから強制的に抜けさせるようにすることで、テスト機能を利用する暗号キーのハックを確実に防止できるようになる。

【0087】

図示実施例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、暗号キーを具体例にして本発明を説明したが、本発明はその適用が暗号キーに限られるものではない。

【0088】

【発明の効果】

以上説明したように、本発明のメモリ装置では、秘匿データが格納されているときには、テスト信号の入力を受け付けないことでテストできないようにする構

成を採ることから、実質的にテスト端子を持たないメモリ装置と同等のセキュリティを実現しつつ、品質向上のためのテストを実行できるようになる。

【0089】

そして、本発明のメモリ装置では、秘匿データに対するアクセス要求の発行を検出すると、それ以降、テスト信号の入力を受け付けなくにする構成を採ることから、実質的にテスト端子を持たないメモリ装置と同等のセキュリティを実現しつつ、品質向上のためのテストを実行できるようになる。

【図面の簡単な説明】

【図1】

本発明の原理構成図である。

【図2】

本発明の一実施例である。

【図3】

ホスト装置とのやり取りの説明図である。

【図4】

本発明の一実施例である。

【図5】

シーケンサの一実施例である。

【図6】

本発明の他の実施例である。

【図7】

本発明の他の実施例である。

【図8】

シーケンサの一実施例である。

【図9】

本発明の他の実施例である。

【図10】

本発明の説明図である。

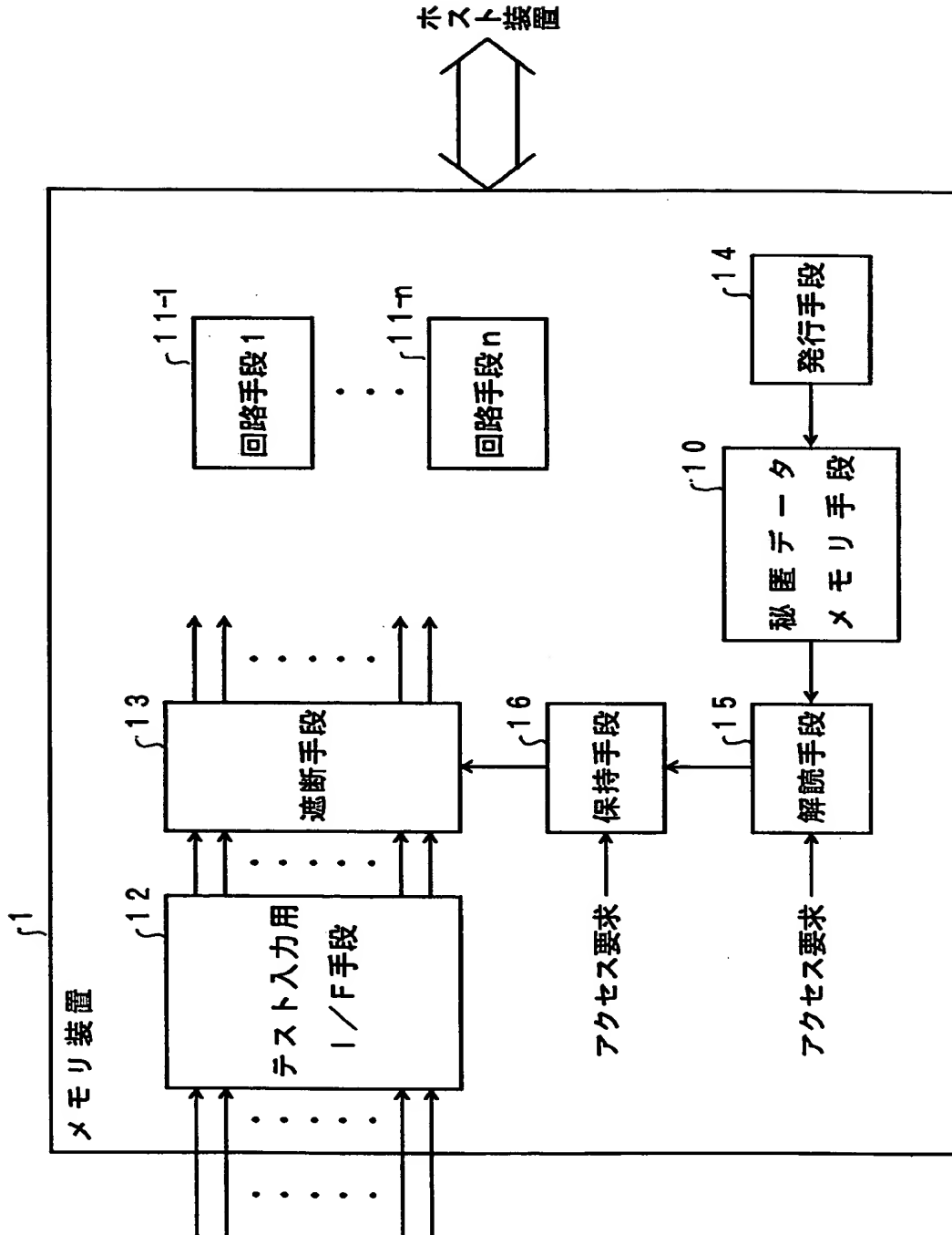
【符号の説明】

- 1     メモリ装置
- 10    秘匿データメモリ手段
- 11    回路手段
- 12    テスト入力用インタフェース手段
- 13    遮断手段
- 14    発行手段
- 15    解読手段
- 16    保持手段

【書類名】 図面

【図 1】

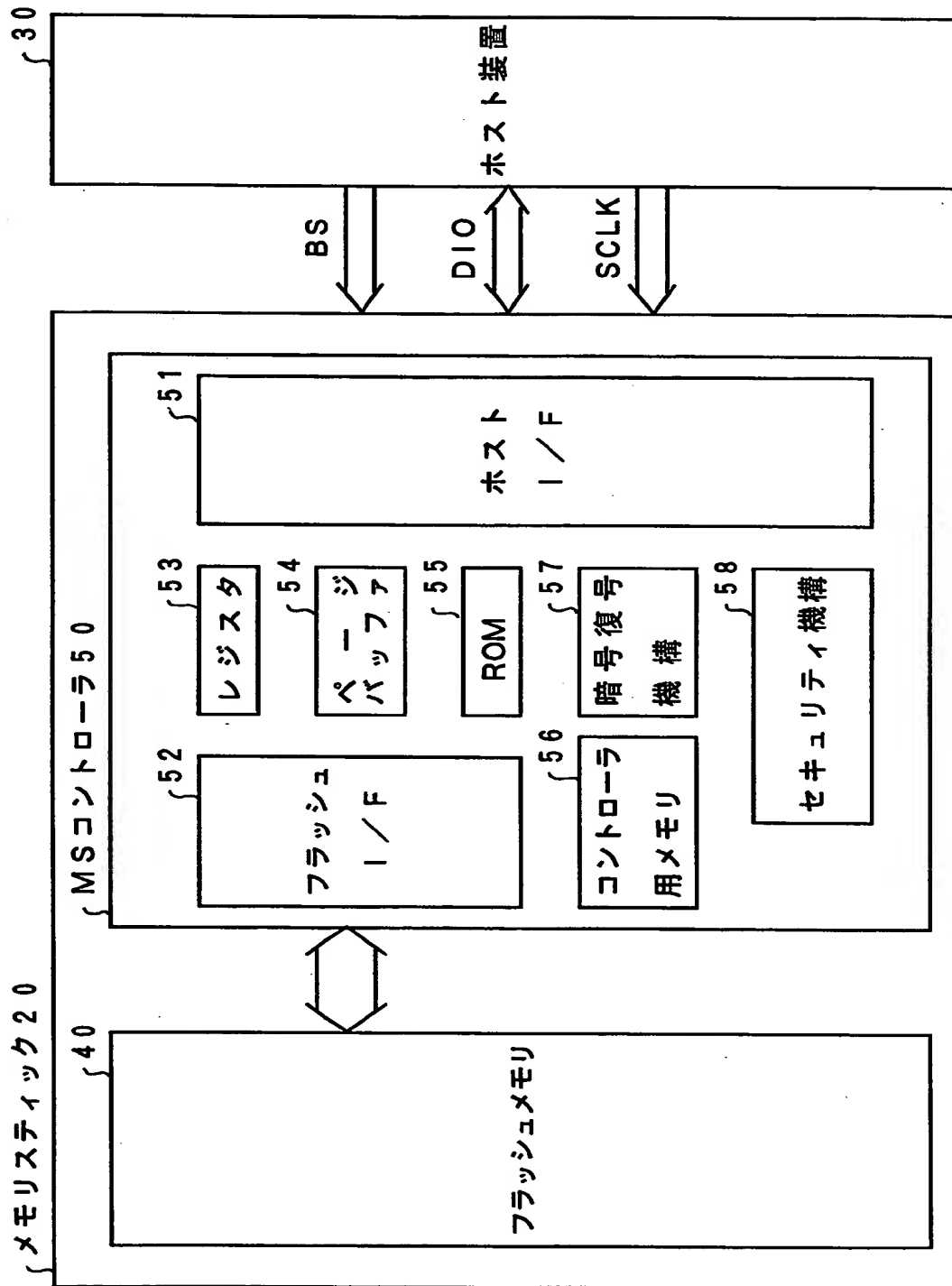
本 発 明 の 原 理 構 成 図





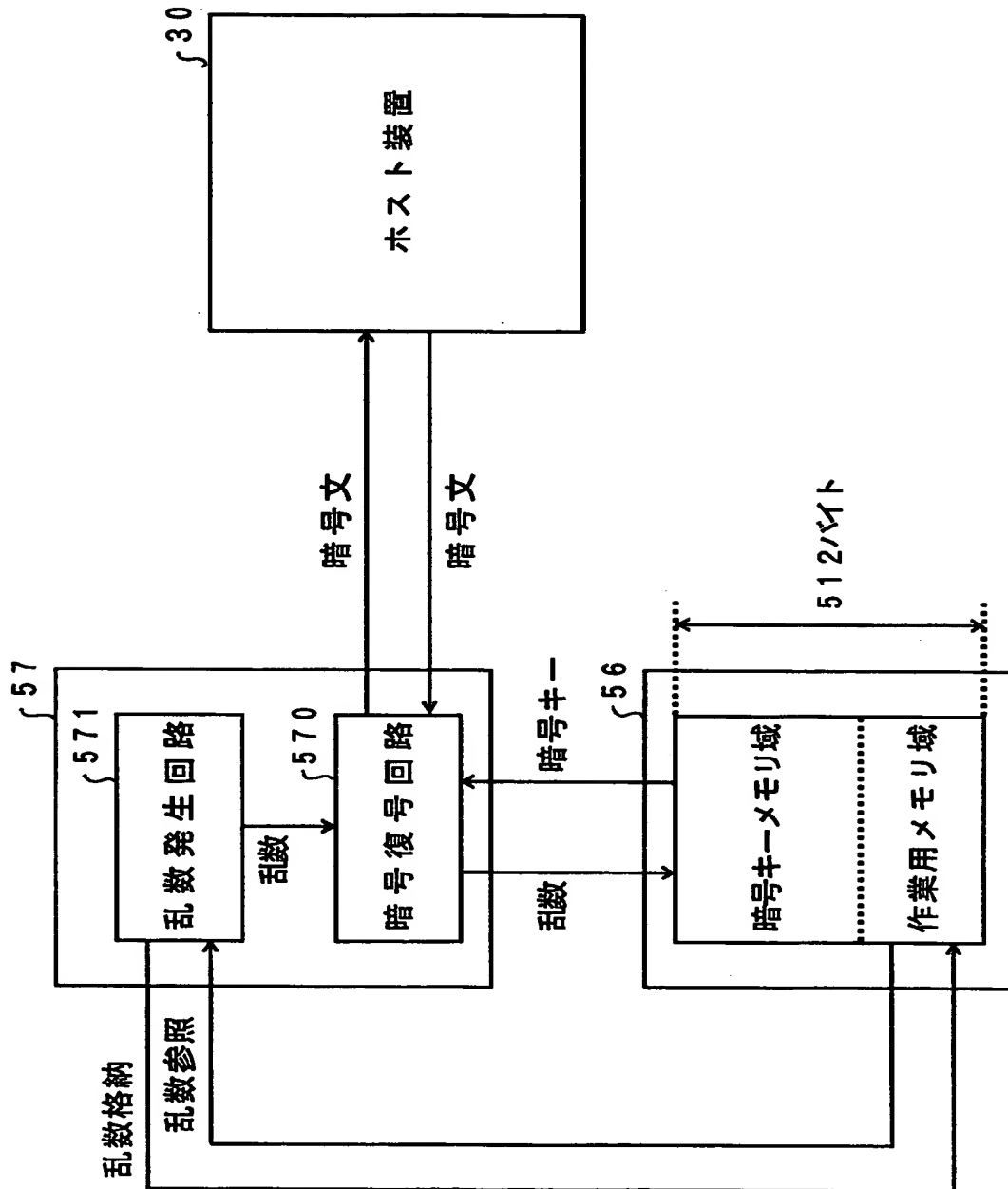
【図 2】

本 発 明 の 一 実 施 例



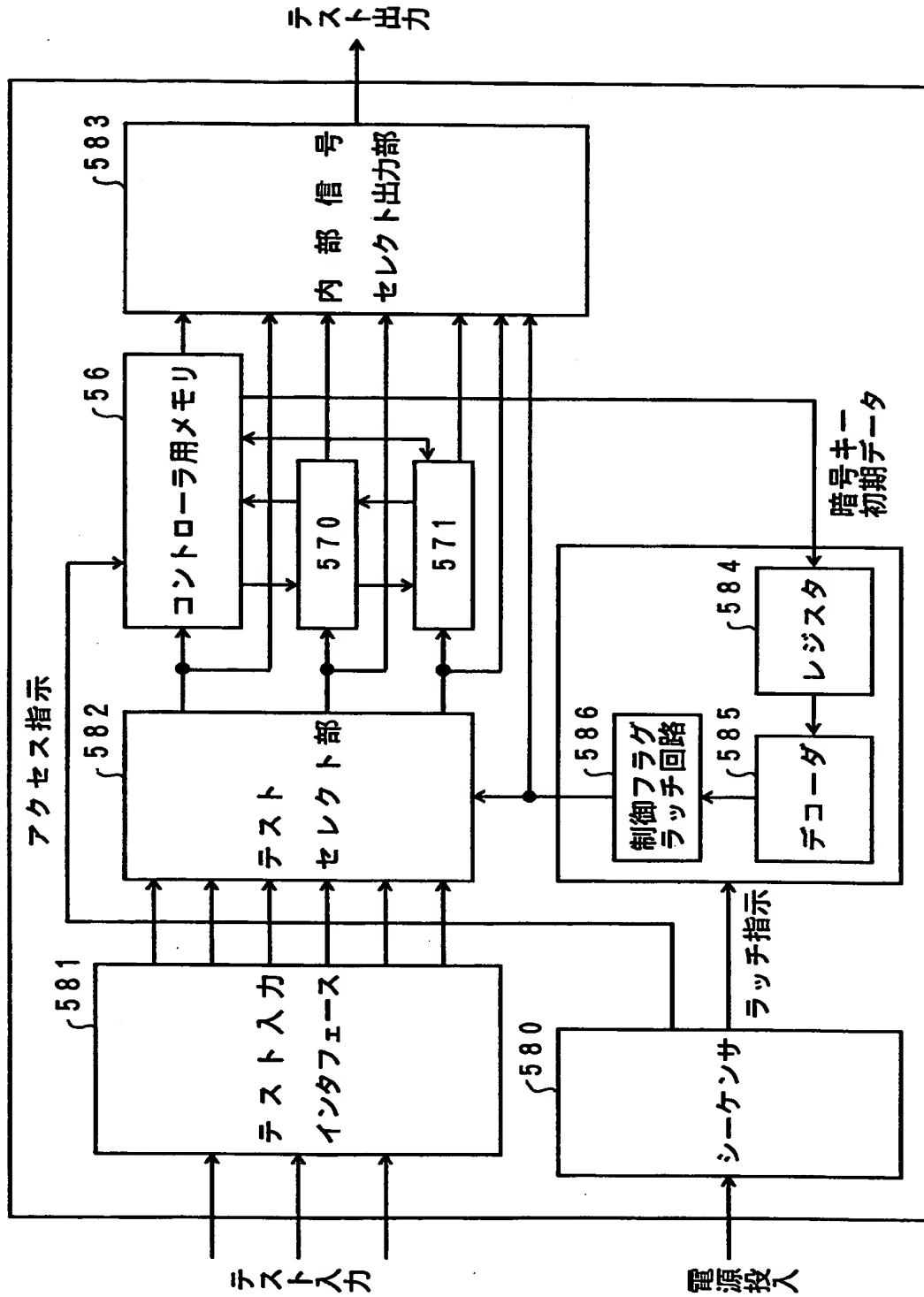
【図 3】

ホ ス ト 装 置 と の や り 取 り の 説 明 図



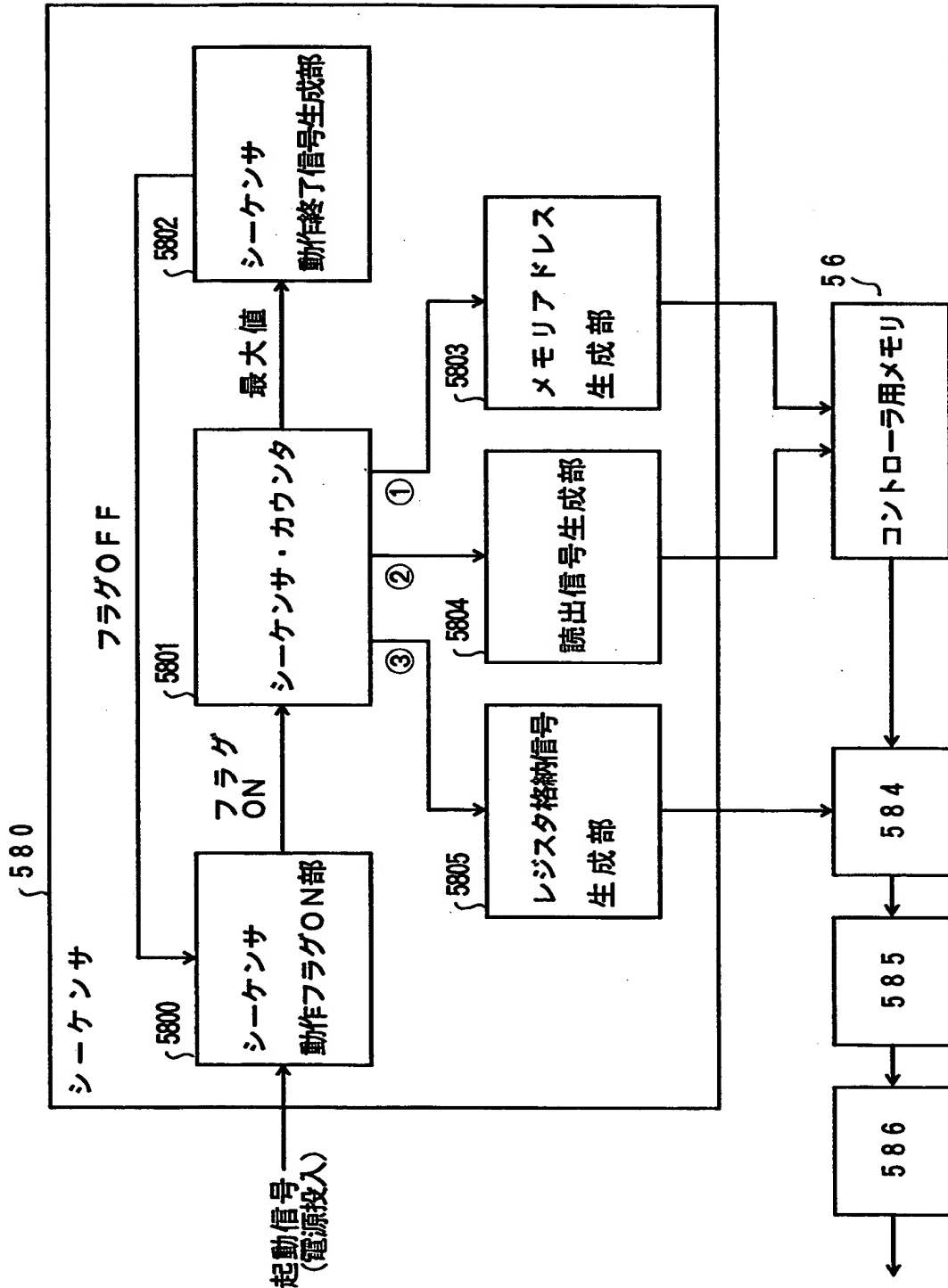
【図4】

本 発 明 の 一 実 施 例



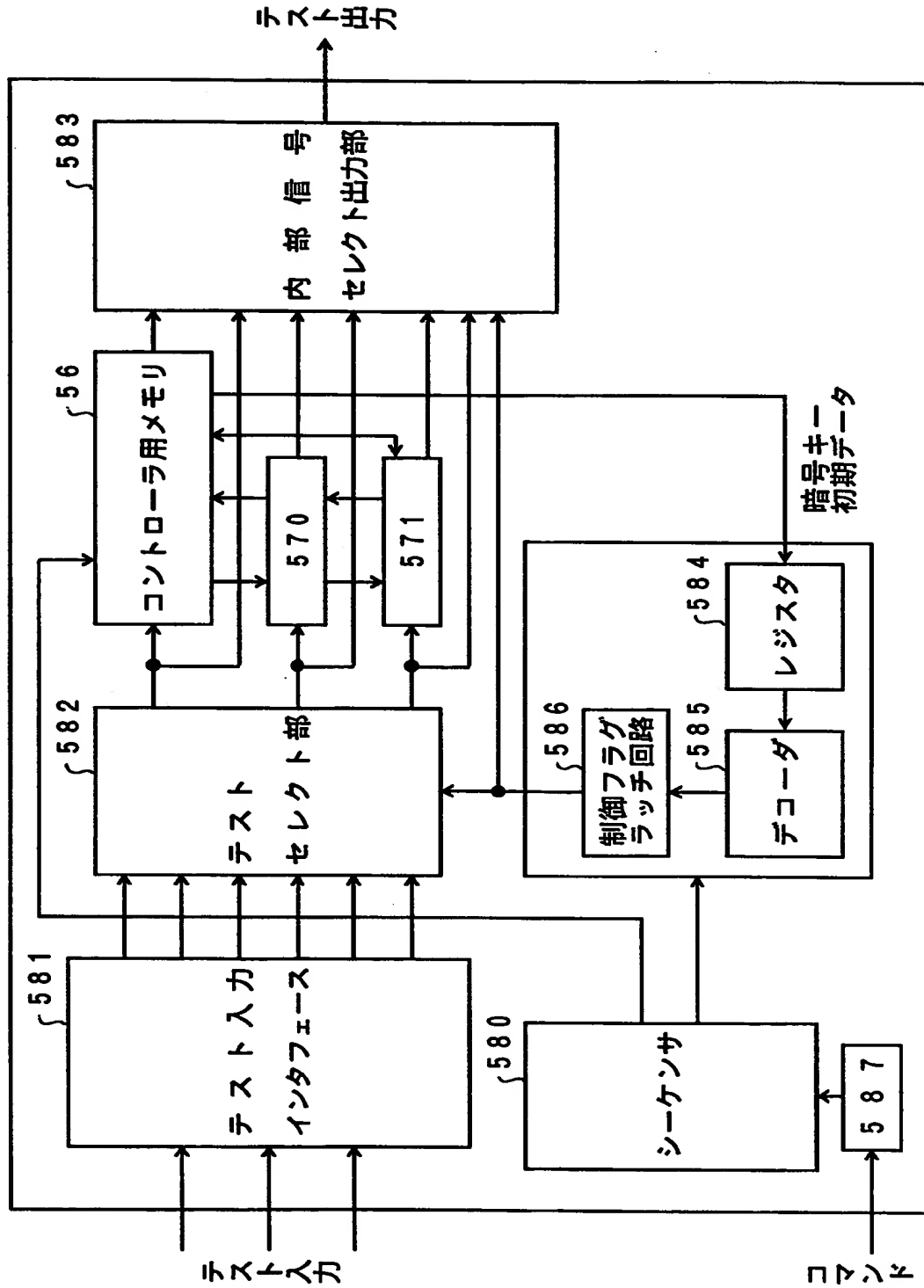
【図 5】

シーケンサの実施例



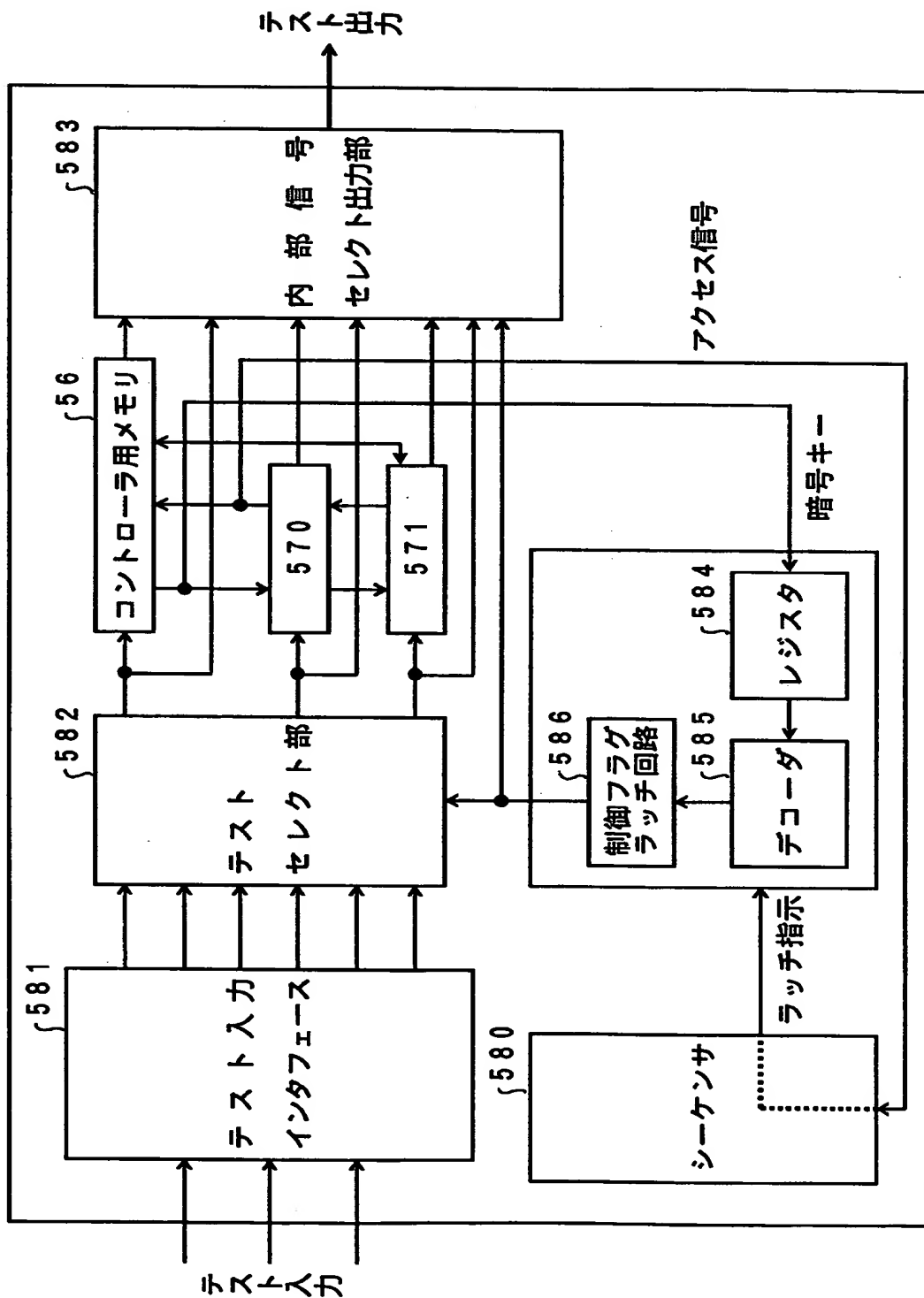
【図6】

本発明の他の実施例



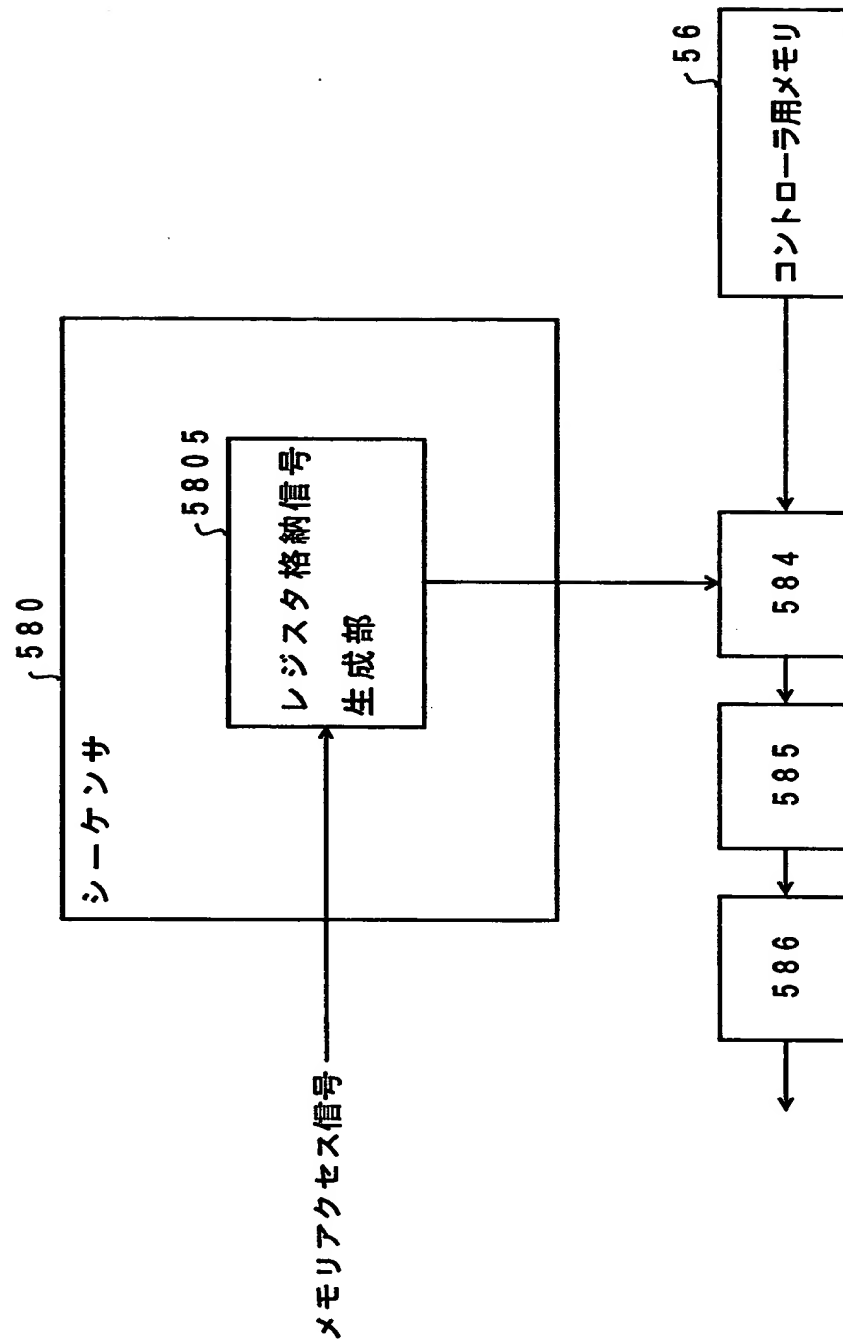
【図 7】

本 発 明 の 他 の 実 施 例



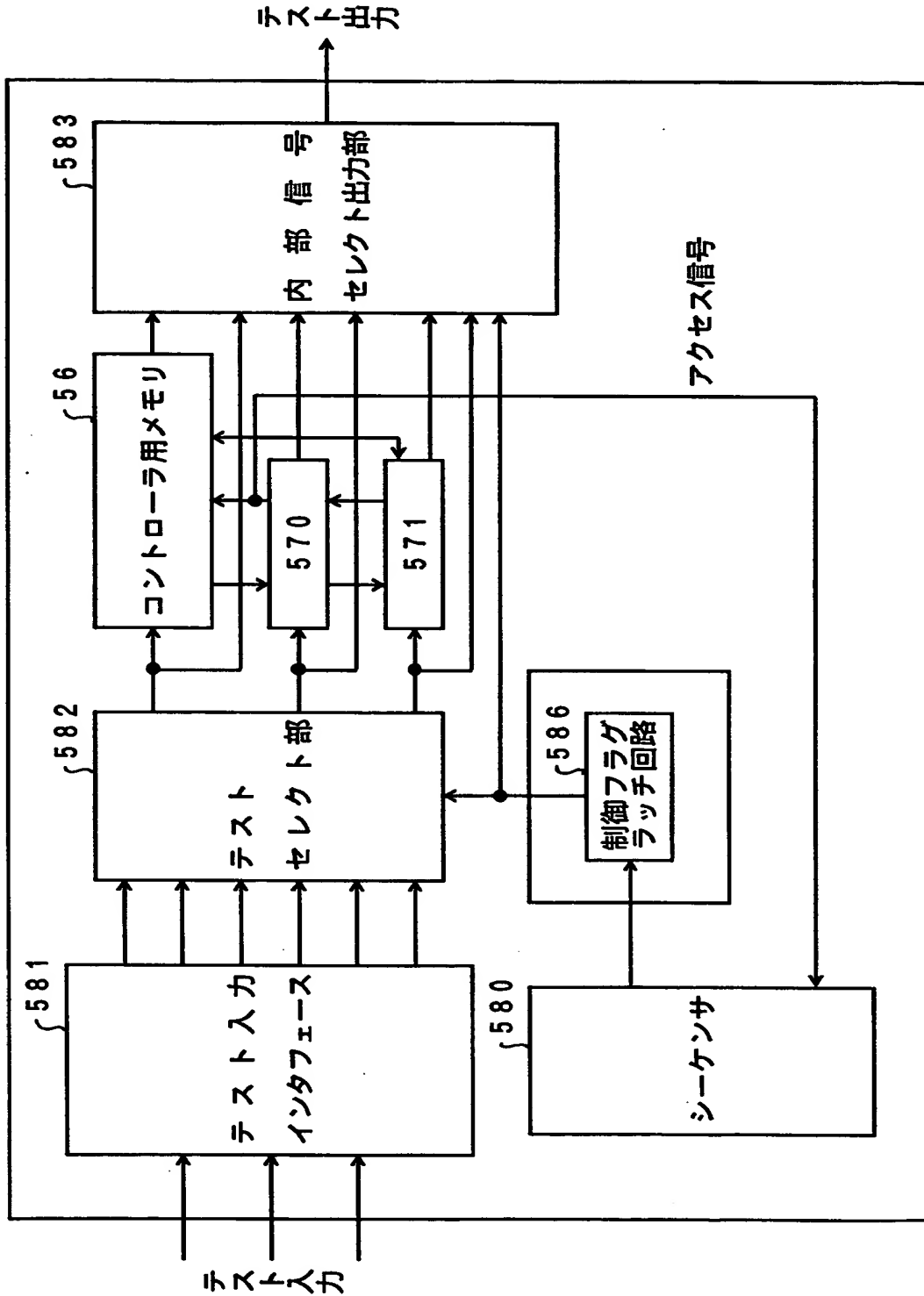
【图 8】

## シーケンサの実施例



【図9】

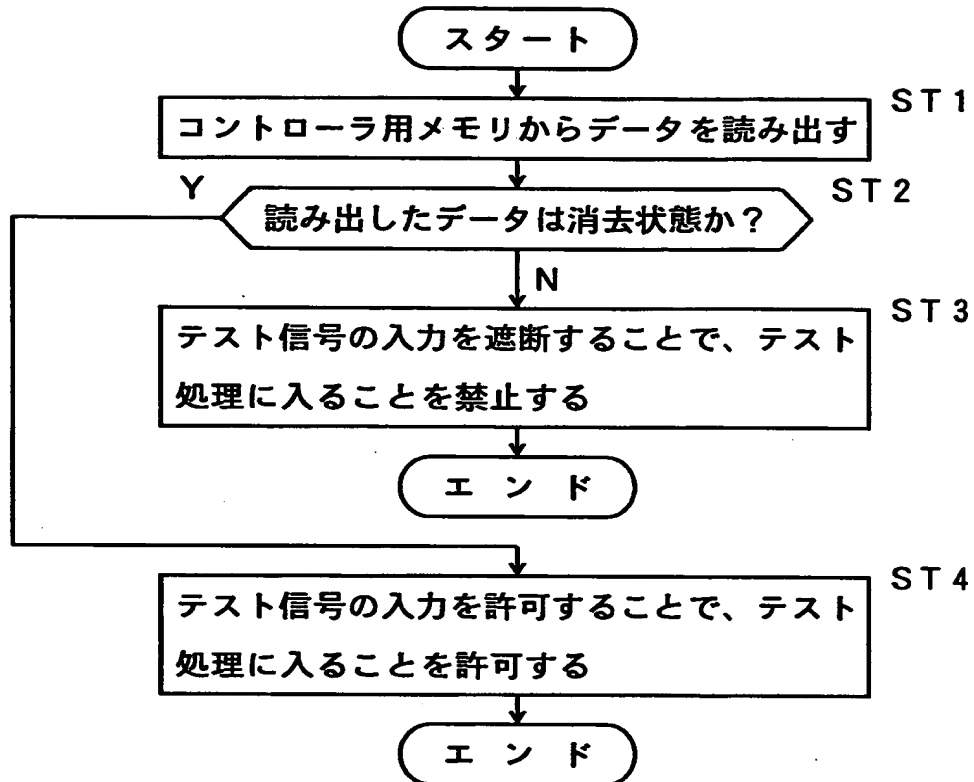
本発明の他の実施例



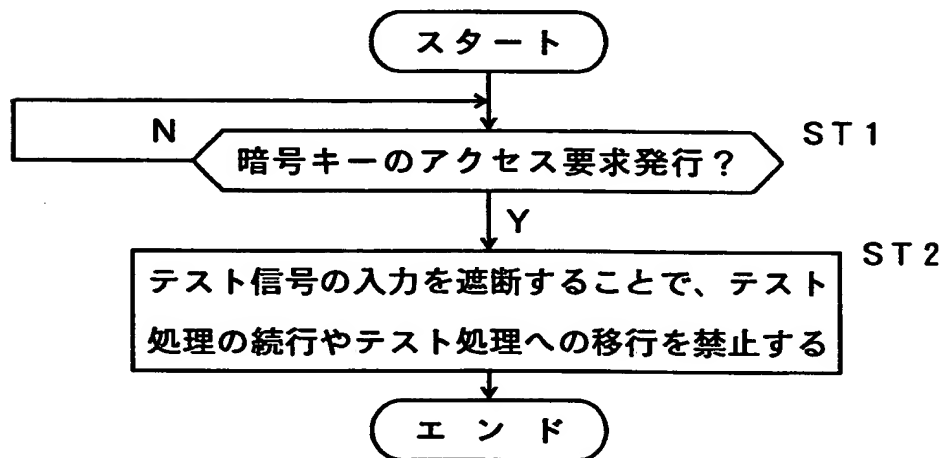


【図 10】

本 発 明 の 説 明 図



(a)



(b)

【書類名】 要約書

【要約】

【課題】本発明は、電源遮断時にもデータを保持するメモリ装置に関し、高いセキュリティを実現しつつ、テスト端子から入力されるテスト信号に従ってテスト処理を実行できるようにすることを目的とする。

【解決手段】秘匿データを格納するメモリ 1 0 に対して、データの読み出し指示を発行する発行手段 1 4 と、発行手段 1 4 の発行処理に応答して読み出されるデータから、秘匿データを格納するメモリ 1 0 に秘匿データが格納されているのか否かを解読する解読手段 1 5 と、解読手段 1 5 の解読結果を揮発性の形態で保持する保持手段 1 6 と、保持手段 1 6 が秘匿データの格納を示す情報を保持するときに、テスト端子から入力されるテスト信号を遮断する遮断手段 1 3 とを備えるように構成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社